Échec de la mise à niveau WSA de SMA en raison d'une configuration SSL non valide

Table des matières

Problème

Lors d'une tentative de mise à niveau d'un appareil de sécurité Web (WSA) à partir de SMA (Security Management Appliance), le processus de mise à niveau échoue avec le message d'erreur « Update failed to upgrade (Motif : Configuration SSL non valide)." La mise à niveau est réussie lorsqu'elle est effectuée directement à partir de l'interface Web WSA, mais échoue systématiquement lorsqu'elle est lancée à partir du SMA. Les tentatives de résolution du problème en générant un nouveau certificat auto-signé et en modifiant le certificat d'authentification par défaut ont échoué.

Environnement

- Appareil de sécurité Web Cisco (WSA)
- Version du logiciel: 15.2.2-009 (MD)
- Appliance de gestion de la sécurité Cisco (SMA)
- Version de mise à niveau cible : AsyncOS 15.5
- Fonctionnalité DNS vérifiée et fonctionnant correctement

Résolution

La résolution implique la désactivation des versions TLS héritées (TLSv1.0 et TLSv1.1) sur l'appliance WSA pour répondre aux conditions préalables de mise à niveau pour AsyncOS 15.5.

Étape 1: Identifier la cause première

L'échec de la mise à niveau est causé par un changement dans le comportement d'AsyncOS 15.5 où TLSv1.0 et TLSv1.1 ne sont plus pris en charge dans aucune configuration SSL autre que la configuration proxy. Le processus de mise à niveau nécessite TLSv1.2 ou une version ultérieure pour les configurations SSL non proxy.

Étape 2: Désactiver les versions TLS héritées

Désactivez TLSv1.0 et TLSv1.1 sur le périphérique WSA via l'interface de configuration. Cette modification satisfait aux conditions requises pour la mise à niveau et permet la poursuite du processus de mise à niveau.

Étape 3: Vérifier la compatibilité des services externes

Assurez-vous que les services externes tels que LDAP prennent en charge TLSv1.2 ou les versions ultérieures. Tant que ces services sont compatibles avec TLSv1.2 et versions ultérieures, la mise à niveau n'interrompt pas la communication avec les systèmes externes.

Étape 4: Procéder à la mise à niveau

Après avoir désactivé les versions TLS héritées, recommencez le processus de mise à niveau à partir du SMA. La mise à niveau peut maintenant se poursuivre sans l'erreur « Invalid SSL configuration ».

Étape 5: Surveiller et valider

Surveillez le processus de mise à niveau pour vous assurer que tous les services dépendants continuent à fonctionner correctement avec TLSv1.2 après la mise à niveau.

Motif

L'échec de la mise à niveau est causé par un changement de comportement introduit dans AsyncOS 15.5.0-566 où TLSv1.0 et TLSv1.1 ne sont plus pris en charge dans aucune configuration SSL autre que la configuration proxy. Cela crée une condition préalable à la mise à niveau qui nécessite de remplacer la version TLS par TLSv1.2 ou ultérieure avant de mettre à niveau AsyncOS. Le processus de mise à niveau SMA effectue des contrôles de validation préalables à la mise à niveau qui détectent cette incompatibilité et empêchent la mise à niveau de se poursuivre.

Autres informations utiles

- Notes de version d'AsyncOS 15.5
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.